学校编码：10384 密级_____
学号： 2006221018

厦门大学

工 程 硕 士 学 位 论 文

企业网络改造及优化的研究和设计

Research and Design of Enterprise Network Transformation and optimization

张少菲

指导教师姓名：吴锦林教授
专 业 名 称：计算机技术
论文提交日期：2010 年 7 月
论文答辩时间：2010 年 12 月
学位授予日期：

答辩委员会主席：
评阅人：

2010 年 12 月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下,独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外,该学位论文为(　　)课题(组)的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　　）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

摘 要

互联网的快速发展使得企业网络成为越来越重要的需求。随着应用水平的提高，企业基于网络的应用早已扩展到电子商务、企业资源存储和共享、网上办公、电子邮件和远程接入等关系到业务运营的应用。良好的企业网络环境可以有效提高企业的运营效率，但是信息安全问题却给许多企业造成了重大损失。

本文针对省内某企业的实际网络环境，通过对企业网现状的调查研究以及与企业信息部门工作人员的交流，得出企业网改造优化的实际需求，并依此设计了整体网络改造方案。企业网的改造优化主要由三部分组成：网络链路、网络安全以及数据存储备份的改造和优化。网络链路的改造主要体现在核心网络设备和链路的冗余备份，以及网络汇聚层交换机vlan的划分和访问控制列表的应用。通过VRRP技术的应用，实现双核心网络设备的冗余功能，避免网络单点故障。网络安全的改造包括企业应用的安全和网络连通的安全。通过硬件安全设备以及相应的安全策略和技术的设定，实现网络安全的目标。企业网外部用户远程接入至企业网内部时，通过采用安全的虚拟专用网络VPN接入，确保传输通道的专用性和安全性，实现安全的远程接入。数据存储备份通过两级数据存储和备份方式（服务器+磁盘阵列），通过备份软件工具和相应的备份策略实现企业信息数据的备份和恢复需求。

企业本次的网络改造和优化设计实现了各项功能要求，在系统改造实施完成后，通过对整体安全功能进行测试，测试结果显示能够提供核心网络冗余、网络安全和数据安全存储备份的功能，达到了预期的安全效果。

关键词：局域网，网络安全，数据存储，数据备份

Abstract

The rapid development of the Internet makes the enterprise network become more and more important. With the raising of the application level of enterprise , network-based applications have been extended to early electronic business, enterprise resource storage and sharing, online office, email and remote access and other applications related to business operations. Good corporate network environment can improve the operational efficiency of enterprises, but information security has given many companies which have brought lots of significant losses.

In this paper, author analysed the enterprise network environment, obtained the actual needs of enterprise network optimization, design the overall network transformation program at last. Network transformation consists of three parts: the network link, network security , data storage and backup. Transformation of the network link is mainly embodied in the core network equipment and redundant backup link, and network aggregation layer switch vlan classification and application of access control lists. By the application of VRRP technology, dual-core network equipment redundancy. Network Security include enterprise applications, security and network connectivity security. Through hardware security devices, security policies and technology, achieve the goal of network security. Remote access to corporate networks to external users within the enterprise network, through the use of secure virtual private network VPN access, to ensure that the dedicated transmission channel and security. To achieve the purpose of data storage backup,we used the two-level way (server + disk arrays) .Using the backup software and tools to achieve enterprise information data backup and recovery needs.

Through this network transformation, the enterprise implements the functional requirements on the network. When the network transformation is complete, the overall security has been tested, and the test result show that the core network could provide redundancy, network security, storage backup and data security features, which achieve the expected safety effect.

Key words: LAN, Network Security, Data Storage, Data Backup

目 录

第一章 前 言

1.1 选题的背景及意义

步入二十一世纪之后，随着社会的进步，人们对灵活、快捷、方便的网络通讯方式要求越来越高，从而极大的刺激了互联网技术的发展。互联网亦成为了当前发展最快、市场前景最大的业务方向。互联网的快速发展使得企业网络成为企业越来越重要的需求，企业网络的建设已经不仅仅是为了建立一个网站对企业进行宣传，或者只是满足员工对互联网的访问。随着应用水平的提高，企业对互联网的应用早已扩大到电子商务、企业资源存储和共享、网上办公、移动办公人员的 VPN 拨入、系统的远程维护等关系到企业日常运行的应用。

企业广泛地利用信息化手段可以提升自身的竞争力，先进的信息设施可以有效提高企业的运营效率，使企业可以更快速的发展壮大。然而在获得这些利益的同时，信息安全问题给许多企业造成了重大损失，已有大量报道和统计资料显示企业正为形形色色的攻击行为付出高昂的代价，而这些被曝光的案例尚只是冰山一角[1]。越来越多的人开始认识到企业中最宝贵的不是各种网络硬件，而是网络中存储的业务数据。在有些单位的信息系统中管理的数据，其数据量大、来源广、种类多、结构复杂、应用广泛。其中很多数据是由几代人积累起来的，有些数据的采集甚至付出了血的代价，所以数据是非常宝贵的财富。系统的崩溃、病毒的入侵、人为的失误，都会造成数据的丢失。数据一旦丢失，将会严重影响企业日常业务的正常运作----丧失商业机会、客户表示不满、营业收入降低、企业声誉受损。此时，最关键的问题就在于如何尽快恢复数据，使系统恢复正常运作。保证数据的安全，就是保证企业的安全。如果企业信息数据的安全得不到保证，那么对网络的大量投资就失去了意义。造成数据安全方面问题的主要原因可分为二大类，一类为存放数据的硬件设备出现故障，另一类是人为因素，如计算机犯罪、计算机病毒、软件错误及人为的误操作。在网络环境下，除了人为的错误操作之外，还有各种各样的病毒感染、系统故障、线路故障和非授权用户入侵等，使企业数据的安全无法得到保障。因此在

企业网络改造和优化的过程中，不仅需要考虑企业网络的可用性，其可靠性和安全性也是必须要考虑的部分。

综上，高效、安全、可靠的企业网络对企业的生存和发展有着至关重要的作用，因此进行企业网络改造和优化的研究具有非常重要的意义。

1.2 国内外研究现状

企业网络属于局域网组网的一种形式。目前局域网通信安全研究采用以广播为技术基础的以太网，任何两个节点之间的通信数据包，不仅为这两个节点的网卡所接收，也同时为处在同一以太网上的任何一个节点的网卡所截取[2]。因此，黑客只要接入以太网上的任一节点进行侦听，就可以捕获发生在这个以太网上的所有数据包，对其进行解包分析，从而窃取关键信息，这就是以太网所固有的安全隐患。事实上，因特网上许多免费的黑客工具都把以太网侦听作为其最基本的手段。

当前，保证局域网安全的解决办法有以下几种：

1．网络分段

网络分段通常被认为是控制网络广播风暴的一种基本手段，但其实也是保证网络安全的一项重要措施。其目的就是将非法用户与敏感的网络资源相互隔离，从而防止可能的非法侦听，网络分段可分为物理分段和逻辑分段两种方式。

目前，一般的局域网大多采用以交换机为中心、路由器为边界的网络格局，应重点挖掘中心交换机的访问控制功能和三层交换功能，综合应用物理分段与逻辑分段两种方法，来实现对局域网的安全控制[3]。例如：普遍使用的 DEC MultiSwitch 900 的入侵检测功能，其实就是一种基于 MAC 地址的访问控制，也就是上述的基于数据链路层的物理分段。

2．以交换式集线器代替共享式集线器

对局域网的中心交换机进行网络分段后，以太网侦听的危险仍然存在。这是因为网络最终用户的接入往往是通过分支集线器而不是中心交换机，而使用最广泛的分支集线器通常是共享式集线器。这样，当用户与主机进行数据通信时，两台机器之间的数据包（称为单播包 Unicast Packet）还是会被同一台集线器上的其他用户

所侦听。一种很危险的情况是：用户 TELNET 到一台主机上，由于 TELNET 程序本身缺乏加密功能，用户所键入的每一个字符（包括用户名、密码等重要信息），都将被明文发送，这就给黑客提供了机会[4]。

因此，应该以交换式集线器代替共享式集线器，使单播包仅在两个节点之间传送，从而防止非法侦听。当然，交换式集线器只能控制单播包而无法控制广播包（Broadcast Packet）和多播包（Multicast Packet）[5]。所幸的是，广播包和多播包内的关键信息，要远远少于单播包。

3．VLAN 的划分

为了克服以太网的广播问题，除了上述方法外，还可以运用 VLAN（虚拟局域网）技术，将以太网通信变为点到点通信，防止大部分基于网络侦听的入侵。

目前的 VLAN 技术主要有三种：基于交换机端口的 VLAN、基于节点 MAC 地址的 VLAN 和基于应用协议的 VLAN。基于端口的 VLAN 虽然稍欠灵活，但却比较成熟，在实际应用中效果显著，广受欢迎。基于 MAC 地址的 VLAN 为移动计算提供了可能性，但同时也潜藏着遭受 MAC 欺诈攻击的隐患。而基于协议的 VLAN，理论上非常理想，但实际应用却尚不成熟。

在集中式网络环境下，通常将中心的所有主机系统集中到一个 VLAN 里，在这个 VLAN 里不允许有任何用户节点，从而较好地保护敏感的主机资源。在分布式网络环境下，可以按机构或部门的设置来划分 VLAN。各部门内部的所有服务器和用户节点都在各自的 VLAN 内，互不侵扰。

VLAN 内部的连接采用交换实现，而 VLAN 与 VLAN 之间的连接则采用三层交换机路由功能实现。无论是交换式集线器还是 VLAN 交换机，都是以交换技术为核心，它们在控制广播、防止黑客上相当有效，但同时也给一些基于广播原理的入侵监控技术和协议分析技术带来了麻烦[6]。因此，如果局域网内存在这样的入侵监控设备或协议分析设备，就必须选用特殊的带有 SPAN（SwitchPort Analyzer）功能的交换机。这种交换机允许系统管理员将全部或某些交换端口的数据包映射到指定的端口上，提供给接在这一端口上的入侵监控设备或协议分析设备。这样既得到了交换技术的好处，又使原有的入侵监控设备或者协议分析设备有了用武之地。

4．防火墙的应用

目前在互联网上大约有将近20%以上的用户曾经遭受过黑客的困扰。尽管黑客如此猖獗，但网络安全问题至今仍没有能够引起足够的重视，更多的用户认为网络安全问题离自己尚远，这一点从大约有40%以上的用户特别是企业级用户没有安装防火墙(Firewall)便可以窥见一斑[7]，而所有的问题都在向大家证明一个事实，大多数的黑客入侵事件都是由于未能正确安装防火墙而引发的。

防火墙正在成为控制对网络系统访问的非常流行的方法。事实上，在 Internet 上的 Web 网站中，超过三分之一的单位内部网络都是由某种形式的防火墙加以保护，这是对黑客防范最严，安全性较强的一种方式，任何关键性的服务器，都建议放在防火墙之后。

1.3 论文结构安排

本课题主要是针对企业网络改造及优化的研究和设计进行探讨。全文共可分为五个章节：

第一章：主要是介绍了企业网络在信息安全方面所面临的问题，阐述本课题的意义，并对国内外对局域网信息安全的研究和发展现状进行概述。最后，介绍本篇论文所研究的内容和章节安排。

第二章：阐述企业网络改造和优化需要用到的一些理论和技术知识，分析各种技术的功能特性和典型应用。

第三章：了解企业网络的现状，进行企业网络改造和优化的需求分析，根据企业的实际需求对整体改造方案进行设计和梳理。

第四章：提出设计方案，实现企业网络的改造和优化，并对实现后的网络进行系统测试和验证，得出结论。

第五章：全文总结。对本文所做的工作进行总结和展望。

第二章 相关理论和技术综述

如何合理地设计网络结构，保证网络整体的安全性、可靠性和可扩展性，这些都是在进行网络设计和改造时应该考虑的问题。以下将对所用到的几种主要技术和理论给予简要介绍。

2.1 网络安全技术

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。 网络安全从其本质上来讲就是网络上的信息安全。从广义来说，凡是涉及到网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域[11]。网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。

通常情况下，系统安全与性能和功能是一对矛盾的关系。如果某个系统不向外界提供任何服务（断开），外界是不可能构成安全威胁的。但是，企业接入国际互联网络，提供网上商店和电子商务等服务，等于将一个内部封闭的网络建成了一个开放的网络环境，各种安全包括系统级的安全问题也随之产生。构建网络安全系统，一方面由于要进行认证、加密、监听，分析、记录等工作，由此影响网络效率，并且降低客户应用的灵活性；另一方面也增加了管理费用。但是，来自网络的安全威胁是实际存在的，特别是在网络上运行关键业务时，网络安全是首先要解决的问题。选择适当的技术和产品，制订灵活的网络安全策略，在保证网络安全的情况下，提供灵活的网络服务通道[12]。采用适当的安全体系设计和管理计划，能够有效降低网络安全对网络性能的影响并降低管理费用。

网络安全的技术手段通常包括以下几种。

物理措施：例如，保护网络关键设备(如交换机、大型计算机等)，制定严格的网络安全规章制度，采取防辐射、防火以及安装不间断电源（UPS）等措施。

访问控制：对用户访问网络资源的权限进行严格的认证和控制。例如，进行用户身份认证，对口令加密、更新和鉴别，设置用户访问目录和文件的权限，控制网络设备配置的权限，等等。

数据加密：加密是保护数据安全的重要手段。加密的作用是保障信息被人截获后不能读懂其含义。防止计算机网络病毒，安装网络防病毒系统[13]。

网络隔离：网络隔离有两种方式，一种是采用隔离卡来实现的，一种是采用网络安全隔离网闸实现的。隔离卡主要用于对单台机器的隔离，网闸主要用于对于整个网络的隔离[14]。

其他措施：其他措施包括信息过滤、容错、数据镜像、数据备份和审计等。近年来，围绕网络安全问题提出了许多解决办法，例如数据加密技术和防火墙技术等。数据加密是对网络中传输的数据进行加密，到达目的地后再解密还原为原始数据，目的是防止非法用户截获后盗用信息。防火墙技术是通过对网络的隔离和限制访问等方法来控制网络的访问权限。

2.1.1 防火墙

防火墙指的是一个由软件和硬件设备组合而成、在内部网和外部网之间、专用网与公共网之间的界面上构造的保护屏障，是一种获取安全性方法的形象说法。它是一种计算机硬件和软件的结合，使 Internet 与 Intranet 之间建立起一个安全网关（Security Gateway），从而保护内部网免受非法用户的侵入，防火墙主要由服务访问规则、验证工具、包过滤和应用网关 4 个部分组成。

防火墙最基本的功能就是控制在计算机网络中，不同信任程度区域间传送的数据流。例如互联网是不可信任的区域，而内部网络是高度信任的区域。以避免安全策略中禁止的一些通信，与建筑中的防火墙功能相似[16]。它有控制信息基本的任务在不同信任的区域。典型信任的区域包括互联网(一个没有信任的区域)和一个内部网络(一个高信任的区域)。最终目标是提供受控连通性在不同水平的信任区域通过安全政策的运行和连通性模型之间根据最少特权原则。

防火墙对流经它的网络通信进行扫描，这样能够过滤掉一些攻击，以免其在目

标计算机上被执行。防火墙还可以关闭不使用的端口。而且它还能禁止特定端口的流出通信，封锁特洛伊木马。一个防火墙（作为阻塞点、控制点）能极大地提高一个内部网络的安全性，并通过过滤不安全的服务而降低风险。由于只有经过精心选择的应用协议才能通过防火墙，所以网络环境变得更安全[18]。如防火墙可以禁止诸如众所周知的不安全的 NFS 协议进出受保护网络，这样外部的攻击者就不可能利用这些脆弱的协议来攻击内部网络。防火墙同时可以保护网络免受基于路由的攻击，如 IP 选项中的源路由攻击和 ICMP 重定向中的重定向路径。防火墙应该可以拒绝所有以上类型攻击的报文并通知防火墙管理员。

通过以防火墙为中心的安全方案配置，能将所有安全软件（如口令、加密、身份认证、审计等）配置在防火墙上[20]。与将网络安全问题分散到各个主机上相比，防火墙的集中安全管理更经济。例如在网络访问时，一次一密口令系统和其它的身份认证系统完全可以不必分散在各个主机上，而集中在防火墙一身上。

通过利用防火墙对内部网络的划分，可实现内部网重点网段的隔离，从而限制了局部重点或敏感网络安全问题对全局网络造成的影响[22]。再者，隐私是内部网络非常关心的问题，一个内部网络中不引人注意的细节可能包含了有关安全的线索而引起外部攻击者的兴趣，甚至因此而暴漏了内部网络的某些安全漏洞。使用防火墙就可以隐蔽那些透漏内部细节如 Finger，DNS 等服务。Finger 显示了主机的所有用户的注册名、真名，最后登录时间和使用 shell 类型等。但是 Finger 显示的信息非常容易被攻击者所获悉。攻击者可以知道一个系统使用的频繁程度，这个系统是否有用户正在连线上网，这个系统是否在被攻击时引起注意等等。防火墙可以同样阻塞有关内部网络中的 DNS 信息,这样一台主机的域名和 IP 地址就不会被外界所了解。除了安全作用，防火墙还支持具有 Internet 服务特性的企业内部网络技术体系 VPN（虚拟专用网）。

典型的防火墙具有以下三个方面的基本特性：

（一）内部网络和外部网络之间的所有网络数据流都必须经过防火墙

这是防火墙所处网络位置特性，同时也是一个前提。因为只有当防火墙是内、外部网络之间通信的唯一通道，才可以全面、有效地保护企业网部网络不受侵害[24]。

根据美国国家安全局制定的《信息保障技术框架》，防火墙适用于用户网络系统的边界，属于用户网络边界的安全保护设备。所谓网络边界即是采用不同安全策略的两个网络连接处，比如用户网络和互联网之间连接、和其它业务往来单位的网络连接、用户内部网络不同部门之间的连接等。防火墙的目的就是在网络连接之间建立一个安全控制点，通过允许、拒绝或重新定向经过防火墙的数据流，实现对进、出内部网络的服务和访问的审计和控制。

（二）只有符合安全策略的数据流才能通过防火墙

防火墙最基本的功能是确保网络流量的合法性，并在此前提下将网络的流量快速的从一条链路转发到另外的链路上去。从最早的防火墙模型开始谈起，原始的防火墙是一台“双穴主机”，即具备两个网络接口，同时拥有两个网络层地址[25]。防火墙将网络上的流量通过相应的网络接口接收上来，按照 OSI 协议栈的七层结构顺序上传，在适当的协议层进行访问规则和安全审查，然后将符合通过条件的报文从相应的网络接口送出，而对于那些不符合通过条件的报文则予以阻断。因此，从这个角度上来说，防火墙是一个类似于桥接或路由器的、多端口的（网络接口>=2）转发设备，它跨接于多个分离的物理网段之间，并在报文转发过程之中完成对报文的审查工作。

（三）防火墙自身应具有非常强的抗攻击免疫力

这是防火墙之所以能担当企业内部网络安全防护重任的先决条件。防火墙处于网络边缘，它就像一个边界卫士一样，每时每刻都要面对黑客的入侵，这样就要求防火墙自身要具有非常强的抗击入侵本领[27]。它之所以具有这么强的本领防火墙操作系统本身是关键，只有自身具有完整信任关系的操作系统才可以谈论系统的安全性。其次就是防火墙自身具有非常低的服务功能，除了专门的防火墙嵌入系统外，再没有其它应用程序在防火墙上运行。

2.1.2 虚拟专用网络 VPN

虚拟专用网（VPN）被定义为通过一个公用网络（通常是因特网）建立一个临时的、安全的连接，是一条穿过混乱的公用网络的安全、稳定的隧道。虚拟专用网是

对企业内部网的扩展。

虚拟专用网可以帮助远程用户、公司分支机构、商业伙伴及供应商同公司的内部网建立可信的安全连接，并保证数据的安全传输。通过将数据流转移到低成本的压网络上，一个企业的虚拟专用网解决方案将大幅度地减少用户花费在城域网和远程网络连接上的费用[29]。同时，这将简化网络的设计和管理，加速连接新的用户和网站。另外，虚拟专用网还可以保护现有的网络投资。随着用户的商业服务不断发展，企业的虚拟专用网解决方案可以使用户将精力集中到自己的生意上，而不是网络上。虚拟专用网可用于不断增长的移动用户的全球因特网接入，以实现安全连接；可用于实现企业网站之间安全通信的虚拟专用线路，用于经济有效地连接到商业伙伴和用户的安全外联网虚拟专用网。

虚拟专用网至少应能提供如下功能：

加密数据，以保证通过公网传输的信息即使被他人截获也不会泄露。

信息认证和身份认证，保证信息的完整性、合法性，并能鉴别用户的身份。

提供访问控制，不同的用户有不同的访问权限。

根据 VPN 所起的作用，可以将 VPN 分为三类：VPDN、Intranet VPN 和 Extranet VPN。

1. VPDN（Virtual Private Dial Network）

在远程用户或移动雇员和公司内部网之间的 VPN，称为 VPDN.实现过程如下：用户拨号 NSP（网络服务提供商）的网络访问服务器 NAS（Network Access Server），发出 PPP 连接请求，NAS 收到呼叫后，在用户和 NAS 之间建立 PPP 链路，然后，NAS 对用户进行身份验证，确定是合法用户，就启动 VPDN 功能，与公司总部内部连接，访问其内部资源。

2. Intranet VPN

在公司远程分支机构的 LAN 和公司总部 LAN 之间的 VPN.通过 Internet 这一公共网络将公司在各地分支机构的 LAN 连到公司总部的 LAN，以便公司内部的资源共享、文件传递等，可节省 DDN 等专线所带来的高额费用。

3. Extranet VPN